Amendment of the Claims

Please amend claims 21 and 22 as indicated below.

1. (Original) A method for authenticating a Web session comprising:

receiving a user ID; computing a message digest of the user ID;

computing an expiration timestamp for the session;

selecting an index number;

combining the message digest and expiration timestamp;

accessing an encryption key using the index number;

encrypting the combined message using the accessed encryption key; and

converting the encrypted message into an ASCII string.

2. (Original) The method of claim 1, wherein the step of combining the message digest and expiration timestamp more specifically includes concatenating the message digest and expiration timestamp.

3. (Original) The method of claim 1, further comprises passing the ASCII string to a remote computer using an FTP (file transport protocol) URL (uniform resource locator) within an HTML (hyper-text markup language) page, the FTP URL being of the form ftp://ID:ASCII@hostname, wherein ID is the user ID and ASCII is the ASCII string.

4. (Original) The method of claim 1, wherein the step of receiving the user ID more specifically comprises receiving the user ID through an HTML (hyper-text markup language) page that is communicated from a remote client browser.

5. (Original) The method of claim 1, wherein the step of computing a message digest of the user ID more specifically comprises computing a four-byte binary value which is an encoded form of the user ID.

6. (Original) The method of claim 1, wherein the step of computing an expiration timestamp more specifically comprises computing an expiration timestamp in Epoch format.

7. (Original) The method of claim 1, wherein the step of selecting an index number more specifically comprises generating a random number within a predefined range of values.

8. (Original) The method of claim 1, wherein the step of accessing the encryption key more specifically comprises retrieving an encryption key from a storage segment containing a plurality of encryption keys, wherein the retrieved encryption key is obtained from a location or position within the storage segment based upon the index number.

9. (Original) The method of claim 1, wherein the step of encrypting the combined message more specifically comprises encrypting the combined message digest and timestamp into an eight-byte binary value.

10. (Original) The method of claim 1, further comprising the step of concatenating the index number to the encrypted message.

11. (Original) The method of claim 1, wherein the step of converting the encrypted message into an ASCII string more specifically comprises using a "printf" command.

12. (Original) The method of claim 1, wherein the step of converting the encrypted message into an ASCII string more specifically includes converting the encrypted message into a hexadecimal value.

13. (Original) The method of claim 10, wherein the step of converting the encrypted message into an ASCII string more specifically comprises converting the encrypted message and the index number into an ASCII string using a "printf" command.

14. (Original) The method of claim 3, further including the step of passing the index number to the remote computer.

15. (Original) The method of claim 14, wherein the step of passing the index number to the remote computer more specifically comprises passing the index number to the remote computer separate from the ASCII string.

16. (Original) The method of claim 14, wherein the step of converting the encrypted message into an ASCII string more specifically comprises converting a combination of the encrypted message and the index number into an ASCII string, wherein the index number is communicated to the remote computer as a part of the ASCII string.

17. (Original) A system for authenticating a transaction comprising:

logic configured to receive a user ID;

logic configured to compute a message digest of the user ID;

logic configured to select an index number;

logic configured to combine the message digest with expiration timestamp;

logic configured to select an encryption key from a plurality of encryption keys using the index number;

logic configured to encrypt the combined message using the selected encryption key; and

logic configured to convert the encrypted message into an ASCII string.

18. (Original) The system of claim 17, further including logic configured to generate an expiration timestamp.

19. (Original) The system of claim 17, further including logic configured to communicate the ASCII string to a remote computer.

20. (Original) The system of claim 17, further including a local memory for storing the plurality of encryption keys.

21. (Currently Amended) A method for authenticating a transaction comprising:

computing a message digest of a user ID;

concatenating the message digest with an expiration timestamp;

selecting an index number;

selecting an encryption key from a plurality of encryption keys using the index number;

encrypting the message digest using the selected encryption key; and

converting the encrypted message into an ASCII string.

22. (Currently Amended) The method of claim 21~~, further comprising: concatenating the message digest with an expiration timestamp,~~ wherein the step of encrypting the message more specifically includes encrypting the concatenated message using the accessed encryption key.

23. (Original) The method of claim 21, wherein the step of selecting the encryption key more specifically includes retrieving the encryption key from a local memory based on the index number.

24. (Original) The method of claim 21, further including the step of communicating the ASCII string to a remote computer.

25. (Original) The method of claim 21, further including the step of communicating the ASCII string to a person through voice communication.

26. (Original) The method of claim 21, further including the step of printing the ASCII string onto a ticket.

27. (Original) The method of claim 26, wherein the ticket is one selected from the group consisting of an airline ticket, a concert ticket, an employee ID card, and an event ticket.

28. (Original) The method of claim 26, wherein the step of printing the ASCII string onto a ticket more specifically includes printing the ASCII string onto the ticket in a form that it may be later electronically scanned for verification.